

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : 11

REMARKS

In the Office Action mailed September 8, 2005, the Examiner objected to claims 7, 13, 16, 57 and 58 for a variety of informalities. The Applicants have herewith amended claim 7 to provide sufficient antecedent basis for the phrase "the access permission security profile. Further, Applicants amended claim 10 to address antecedent basis directly within claim 10 for the phrase "the access permission security profile" and indirectly within claim 16, as noted by the Examiner. Claims 57 and 58 were also revised to reflect the cancellation of claims 23, 32, and 46 in the previous restriction requirement. Accordingly, it is respectfully requested that these objections be withdrawn.

Regarding substantive rejections, the Examiner rejected Claim 1-20 and 52-57 under 35 USC 103(a) in view of Scheidt (US Pat. 6,490,680) in view of Schwartz (Schwartz, John "Techway, For a Switch, the Code Knows You: A Vienna Firm is Offering a High-Tech Twist: Selective Encryption.") The Examiner broadly referenced several portions of Scheidt with respect to claim 1 yet admitted that Scheidt "does not disclose that this is done on a decentralized public network". Unfortunately, Scheidt alone or in combination with the Schwartz reference does not teach this aspect or several other aspects of claim 1 as recited. For at least this reason, the Examiner has failed to establish a prima facie case for rejecting claim 1. Under MPEP §2143 Basic Requirements of a Prima Facie Case of Obviousness specifies:

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : 12

“To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure. In re Vaeck , 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)”

Accordingly, the Applicants respectfully requests that the Examiner withdraw the rejection under 35 USC 103(a) for failing to teach or suggest each and every claim limitation.

First, it is not clear that Scheidt or Schwartz teaches or suggests any of the limitations in claim 1. For example, Scheidt fails to disclose “receiving a request for an access permission security profile on behalf of a network user” as recited in claim 1. Contrary to the Examiner’s assertion, no where does Scheidt indicate that a network user makes any requests for the access permission security profile. Instead, Scheidt insists that either a smart card (Col. 11, lines 24-30) or a super card (Col. 11, lines 65-67; Col. 12, lines 1-11) should be used store and hold this information and be directly connected to a workstation (i.e., not accessed over a network). There is no request for the access permission security profile since it is already stored in the smart card attached directly to the workstation (Col. 5, lines 65-67; Col. 6, lines 1-6; Col. 10, lines 28-42).

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : 13

Moreover, Scheidt suggests and therefore teaches away from using anything but a smart card. Specifically, Scheidt extolls the virtue of centralizing more tasks to the super card rather than less. It is the teachings, suggestions and belief of Scheidt that placing more functions on the smart card will inherently increase the overall security of the CKM system because “local processing within the card increases the workload of an adversary who is trying to snoop the internal workings” of CKM (Col. 12, lines 1-11). In fact, Scheidt neither recognizes or mentions any of the pitfalls of requiring a physical smart card to perform CKM hence there is clearly no motivation to eliminate this aspect of Scheidt or combine with any other approach.

Scheidt could also not possibly teach or suggest “creating the access permission security profile, to be used in forming a cryptographic key for enabling the network user to decrypt selected portions of an encrypted object and to encrypt selected portions of a plaintext object” as recited in claim 1. First, Scheidt assumes the smart card already has the access permission security profile hence there is no reason to then create it on demand since “the Credential Manager will initialize a smart card with that user’s ID” and the “[the] card is then given to the user.”(Col. 9, lines 39-43). Clearly, the access permission security profile in Scheidt is created in advance and not on demand as recited in claim 1.

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : 14

Further, Scheidt does not teach or suggest “securely transmitting the access permission security profile to the network user over the network” as recited in claim 1. By design, Scheidt stores the access permission security profile on the smart card or super card in advance and then gives the smart card to the user. Once again, Scheidt neither teaches nor suggests this aspect of the invention as recited in claim 1.

Even if these limitations were present, the Examiner has admitted that Scheidt does not in fact teach or suggest providing these functions over “a decentralized public network” as also recited in claim 1. Unfortunately, Schwartz also does not teach or suggest this or any other limitation in claim 1. Schwartz is merely an excerpt from the reporter’s article on the system that Scheidt has created and some of the features this reporter had found interesting. For example, Schwartz mentions that different portions of a document can be encrypted to display different information for different parties. Applicants respectfully submit to the Examiner that this relates to symmetric encryption but not the details of key management. In fact, Schwartz mentions that the user’s information is stored on “smart cards” hence key management in Schwartz is identical to that in Scheidt. This makes sense as Schwartz is a staff reporter from the Washington Post reporting on the details of Scheidt’s company and technology; Schwartz is merely reporting on the technology and not suggesting ways to change or improve it.

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : 15

Indeed, Schwartz mentions on page 2, lines 1-5 when “the information is received on a Web page, the system can even redraw the page to accommodate the information it allows to go out” but this has little to do with the steps recited in claim 1. Once again, this feature mentioned in Schwartz relates to encrypting the web page with multiple different symmetric keys. The fact that the web is a “decentralized public network” is not sufficient to teach or suggest any or all of the aspects of the invention as recited in claim 1.

Even if there were a motivation to combine Scheidt with Schwartz, the combination would not yield any or all aspects of the invention recited in claim 1. By the Examiner’s admission and the aforementioned reasons, Scheidt does not teach or suggest claim 1. At best, Schwartz is merely describing the technology that Scheidt has already created and/or patented using smart cards for key management. For this additional reason, it is therefore is not possible that the combination of Schwartz with Scheidt could yield more than disclosed by Scheidt alone.

Because the Examiner has failed to show each and every element in Scheidt and/or Schwartz, Applicants respectfully request withdrawal of the rejection for claim 1. Independent claim 7 remains patentable for at least the reasons provided with respect to claim 1. Dependant claims 2-6 and 8-22, while allowable on their own, also are in condition for allowance for at least the same reasons specified with respect to claim 1 and/or claim 7 respectively. (“If an independent claim is

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : 16

nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious.” *In re Fine*, 837 F.2d 1071, ___, 5 USPQ2d 1596 (Fed. Cir. 1988)).

The Examiner has also rejected 52-57 under 35 USC 103 over Scheidt. Applicants respectfully submit that Scheidt does not teach or suggest a system having “a plurality of member tokens for providing cryptographic capabilities to authenticated users of the decentralized public network” as recited in claim 52. As previously described, Scheidt describes using a smart card or super card to store this information in advance (Col. 9, lines 39-54) rather than distribute over a network. The Examiner supports this assertion and admits that Scheidt does not teach or suggest a method or system for distributing cryptographic capabilities over a decentralized public network. Unfortunately, Schwartz also does not teach, suggest or even describe any details related to key management or distributing cryptographic capabilities over a decentralized public network for at least the reasons previously described.

Additionally, Scheidt does not teach or suggest “a set of server systems for managing the distribution of the member tokens” as recited in claim 52. Scheidt uses smart cards to hold tokens and does not distribute them using a set of server systems. Scheidt also does not have a “means for requesting a member token from at least one server system” as recited in claim 52 since there is no need to deliver tokens already stored on smart cards. Finally, Scheidt does not provide a “means for

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : 17

securely distributing a requested member token from at least one server system to at least one client system over the decentralized public network” as recited in claim 52 as the tokens are stored on a smart card. Consequently, dependant claims 53-57 remain patentably distinct on their own as well as based upon their dependance on allowable claim 52.

The Examiner also rejected claims 21, 22 and 58 under 35 USC 103 over Scheidt in view of Schwartz and further in view of Anderson (US Pat 5,805,674). First, claim 1, claim 7 and claim 52 remain patentable for at least the reasons specified previously as the Examiner has not established a prima facie case of obviousness. Consequently, dependant claims 21, 22 and 58 remain patentably distinct on their own as well as based upon their dependance on allowable claims 1, 7 and 52 respectively.

While Anderson may describe use of timing and geographic position for authentication, it is in the context of voice recognition and roaming phone calls with a cell phone (Col. 12, lines 1-5). Unfortunately, the timing and geographic position information in Anderson is not related to the timing as recited in claim 21 and the geographic position data as recited in claim 22.

Moreover, there is no motivation to combine the cellular phone network in Anderson with the other references – except by impermissibly using Applicants’ disclosure. In order to rely on a reference as a basis for rejection of the applicant's invention, the reference must either be in the field

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : 18

of the applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned. (See *In re Deminski*, 796 F.2d 436, 442, 230 USPQ 313, 315 (Fed. Cir. 1986). We have reminded ourselves and the PTO that it is necessary to consider "the reality of the circumstances", *In re Wood*, 599 F.2d 1032, 1036, 202 USPQ 171, 174 (CCPA 1979) -- in other words, common sense -- in deciding in which fields a person of ordinary skill would reasonably be expected to look for a solution to the problem facing the inventor." *Id.* at 1447 and "The combination of elements from nonanalogous sources, in a manner that reconstructs the applicant's invention only with the benefit of hindsight, is insufficient to present a *prima facie* case of obviousness. There must be some reason, suggestion, or motivation found in the prior art whereby a person of ordinary skill in the field of the invention would make the combination. That knowledge can not come from the applicant's invention itself." *Diversitech Corp. v. Century Steps, Inc.*, 850 F.2d 675, 678-79, 7 USPQ2d 1315, 1318 (Fed. Cir. 1988); *In re Geiger*, 815 F.2d 686, 687, 2 USPQ2d 1276, 1278 (Fed. Cir. 1987); *Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 1147, 227 USPQ 543, 551 (Fed. Cir. 1985). *Id.* at 1447.) In this case, Anderson concerns voice recognition on a cellular network and aspects of the present invention concerns key management and delivering cryptographic capabilities over a network.

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : 19

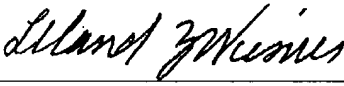
In summary, Applicants respectfully request reconsideration of withdrawal of the rejections for claims 1-22 and 52-58.

The Applicant has made a diligent effort to place the claims in condition for allowance, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Leland Wiesner, Applicants' Attorney at (650) 853-1113 so that such issues may be resolved as expeditiously as possible.

For these reasons provided above, this application is now considered to be in condition for allowance and such action is earnestly solicited.

Respectfully Submitted,

January 9, 2006
Date



Leland Wiesner
Attorney/Agent for Applicant(s)
Reg. No. 39424

Wiesner and Associates
366 Cambridge Ave.
Palo Alto, California 94306
Tel. (650) 853-1113